REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated January 23, 2006. Claims 1-26 are pending. Claims 1-26 are rejected. Claims 16 and 24 have been amended. Accordingly, claims 1-26 remain pending in the present application.

This response is submitted in accordance with Rule 116 in an earnest effort to put the application in better condition for allowance. It is believed that Applicant's response has not amended the claims in a way that would raise new issues for consideration or that would require further searching of the prior art on the part of the Examiner. Arguments are also presented below that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by the arguments, it is respectfully requested that the Examiner enter the Amendment to clarify issue issues upon appeal.

The specification has been amended to update related application information, correct typographical errors and to insert recitations from the Summary and Claims near the beginning of the Detailed Description to improve introductory descriptions of the preferred embodiments. Accordingly, no new matter has been entered.

Claims 16 and 24 have been amended to change the formatting of reference characters enumerating claim elements. These amendments are seen by Applicant as broadening or cosmetic, and as such, are not subject to the prosecution history estoppel imposed by Festo.

Applicant acknowledges and regrets that some errors and misstatements were inadvertently made in the previous Office Action. The remarks herein are intended to replace the remarks made in the previous office action in their entirety for clarification of

the record.

In the Final Office Action, the Examiner rejected claims 1-26 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,898,706 (Venkatesan). Applicants respectfully disagree. Anticipation requires that a prior art reference disclose each and every claim element of the claimed invention. It is respectfully submitted that Venkatesan fails to disclose each in every claim element of the independent claims.

The present invention provides a method and system for the delivery of secure software license information to authorize the use of a software product, such as a software program or software resource. The system includes a software product executing on a computer, and a key authority and/or license server connected to the computer system over a network. The software product includes both a software program and an authorizing program that authorizes use of the software product.

One of the underlying features of the present invention is the delivery of secure software license information between the software product and the key authority through the use digital certificates and digital signatures. According to a preferred embodiment, a publisher certificate and a product certificate are associated with the software product to be authorized, wherein both the publisher certificate and the product certificate include respective private/public key pairs, and wherein at least one of the product certificate private and public keys is digitally signed by the publisher private key associated with the publisher certificate. In a further embodiment, the publisher certificate is digitally signed by a certificate authority. When the software product is invoked, the authorizing program generates a license request containing user and product information. In one embodiment, the license request is secured when transmitted to the key authority and/or license server by digitally signing the license request with the

product private key associated with the product certificate. The key authority and/or license server validates the requests and then generates a license with license terms using data extracted from the license request, digitally signs the license with the publisher private key associated with the publisher certificate, and transmits and the signed license back to the authorizing program. The authorizing program then validates the signed license using the publisher public key, and uses the license terms to control the use of the software product.

Referring now to independent claims 1 and 12, the method for delivering secure license terms to a software program refers broadly to private and public key pairs, rather than to certificates, which usually include other information besides keys. According to the preferred embodiment, the product key is connected to the publisher key so that only that publisher can allow the product to be authorized. To accomplish this, at least one of the product keys is digitally signed by the private key of publisher. Using the public key of the publisher, the authorization program can verify that the publisher who signed the product public key associated with a software product is the same publisher who signed the license in response to license request.

In independent claims 16, Applicants refer to signed certificates, which have associated private keys. The public keys are part of the certificate. So in this case, the product certificate is digitally signed by the publisher private key. This allows the authorization program to verify that the publisher who signed its product certificate is the same publisher who signed the license.

In independent claim 24, a certificate authority that also has a certificate (i.e., a private/public key pair) is recited. The publisher certificate, which contains the publisher public key, is signed by the certificate authority private key. This means that the

protected software program can not only verify that it was authorized by the correct publisher, but can also verify that the publisher is certified by the certificate authority.

In a further embodiment, the publisher of the software program can use a toolset to convert the software program into a license-managed product. The certificate Authority certificate is used to issue a publisher certificate to a publisher, and the publisher certificate is used to regulate license terms for using the toolset. The publisher uses the toolset and the publisher certificate to create protected software products and to create product certificates for licensing.

Thus, the present invention provides a chain of certificates to authorize use of a software program through a license. To run, a software product has to verify the certificates. Verification means verifying the certificate chain, meaning that the product certificate is cryptographically tied to the proper publisher certificate, which in turn according to a further embodiment, must be cryptographically tied to the certificate authority certificate. The elegance of the solution is that it allows the certificate authority to control how publishers use the toolset, allows publishers to control how their end-users use their protected software products, and prevents one publisher from authorizing a product from another publisher.

Thus, the claims of the present invention are directed to methods for *securely delivering license information*, including the initial license request, between a software product and a key authority through a chain of certificates associated with the software product. In contrast, Venkatesan is directed to techniques for controlling access and use of protected objects by client computer using a digital rights management (DRM) system in the client computer that is based primarily on watermarks being embedded throughout the software object.

In the previous Office Action, Applicant mistakenly stated that Venkatesan fails to teach or suggest a software licensing mechanism; fails to teach or suggest associating a public and private key pair with a software publisher; fails to teach or suggest generating a license using data extracted from the license request and license terms; and fails to teach or suggest preventing use of the software product on a different computer than that used to generate the license request. Applicant retracts those statements and acknowledges that Venkatesan teaches a software licensing mechanism and the association of a public and private key pair with a software publisher. Venkatesan also teaches that the publisher cryptographically signs the license in response to a license the request.

However, despite these teachings, Venkatesan still fails to address the security of the license request and resulting license, as claimed in the present invention for least the following reasons. First, although Venkatesan may teach associating a private and public key pair with a software publisher, Venkatesan fails to teach or suggest a software product that "includes a software program and *an authorization program within* the software product," as recited in step (a) of claim 1, where "upon invocation of the software product on a computer," the authorization program generates "a license request," as recited in steps (c) and (c)(i) of claim 1.

Venkatesan fails to teach or suggest that the software object, or part thereof, that has been downloaded to a client PC generates a license request. Instead, Venkatesan clearly teaches that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser). Example portions of Venkatesan state:

> After a user has downloaded a watermarked object, then, in order to use that object, the user, through his(her) client PC, electronically transacts, through the Internet, with publisher's web server. In return for

payment of a specific licensing fee to the publisher, this web server downloads to the client PC an electronic license… (Col. 6, lines 21-27) and (col. 14, lines 35 and 41).

Subsequently, the user, through client PC_j, establishes an Internet session with the publisher's web server and as, indicated by block 540, electronically transacts with that server to obtain a license to use the previously downloaded object.... Once the user makes the selection and authorizes electronic payment for the desired rights, the browser, based on embedded code in the web page, transmits, to the publisher's web server, the rights selection, payment authorization and a computer identification (CID) associated with client PC_j.... Once this information is transmitted to the publisher's web server, that server issues, as indicated by block 550 shown in FIG. 5, an electronic license (L_i) and transmits, as symbolized by line 555, that license to the client PC. (Col. 21, line 66 through col. 22, line 20).

Accordingly, because the generation of the license request is manually initiated by the user by interacting with the PC through a Web browser, Venkatesan fails to teach or suggest that the software object or a part thereof generates the license request upon invitation of the software object.

It should be noted that Venkatesan also provides for an enforcer that looks for watermarks in an object whenever the client computer attempts to access a file containing the protected object. It is also believed that the enforcer cannot be considered analogous to the "authorization program" because the enforcer does not generate a license request. In addition, the enforcer is not part of the protected software object. Rather, the enforcer is part of a digital rights management (DRM) system, which in turn is part of the operating system (col. 18. lines 44-45).

Consequently, Venkatesan's fails to teach or suggest a software product that "includes a software program and *an authorization program within* the software product," where "upon invocation of the software product on a computer," the authorization program generates "a license request," as recited in claim 1.

Second, although Venkatesan may teach the use of a publisher key, Venkatesan also fails to teach or suggest "associating a *product* private key and public key with the software product", as recited in step (b) of claim 1. On page 7 of the Final Office Action, the Examiner cites figure 5, step 550, of Venkatesan for teaching this step, stating "upon payment by user, publisher issues and downloads to user electronic license with usage rights including secret key." However, nothing pertaining to step 550 teaches or suggests associating a product private and public key pair with a software products/object. The Examiner makes reference to a "secret key", but Venkatesan describes that this secret key, which is included in the license, "is to decrypt the [software] object. This secret key..., is a symmetric encryption key, i.e., the same key used use by the publisher to encrypt the object (col. 22, lines 25-28). Although Venkatesan's secret key is used to encrypt the software object, and presumably considered by the Examiner to be "associated" with the software object, Venkatesan's secret key is "symmetric", i.e., there is only one. Consequently, there can be no pair of product keys, i.e., a product private key and public key. More importantly, it is believed that Venkatesan's secret key is only used to encrypt and decrypt the software object, but not to "digitally sign the license request," as explained further below.

In addition, contrary to the Examiner's assertion during the rejection of claim 3, it is also believed that Venkatesan's product identification (PID) and certified public key also fail to teach or suggest the claimed product key for the following reasons. First, Venkatesan's product identification (PID) is defined as a value (col., line 64), not as a cryptographic key; and unlike the claimed product key, the PID is not used to digitally sign anything, let alone the license request. Second, the certified public key referred to by the Examiner in step 1122 of Venkatesan also fails to teach or suggest the claimed

product key because the certified public key is associated with the client PC, not the software object (col. 30, lines 31-34). Although the certified public key is used to encrypt the license after being provided to the publisher by the client PC as part of the license request, this key is public, not private, and is not used to sign or encrypt the license request, as the claimed product key.

Furthermore, because Venkatesan fails to teach associating a product public key and private key with a software product, Venkatesan cannot teach "digitally signing" "at least one of the product private and public keys with the publisher private key", as recited in step (b) of claim 1.

One of the elements of the present invention is the fact that the license request generated by the authorization program is delivered securely to the key authority. The security is provided by "digitally signing the license request with the product private key," as recited in step (c) (ii).

Not only does Venkatesan fail to teach or suggest that some part of the software object that has been downloaded to a client PC generates a license request, as described above, Venkatesan also fails to address providing security for the license request. Venkatesan merely describes that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser), and in return receives a license. Not only is Venkatesan's license request not signed by a product private key, but the license request appears not to be signed or encrypted all. Consequently, Venkatesan fails to teach or suggest "digitally signing the license request with the product private key," as recited in step (c) (ii).

In the Response to Arguments section of the Final Office Action, the Examiner took issue with Applicant's statement in the previous Amendment that unlike the

present invention, in Venkatesan, there is no chaining of certificates. To rebut this argument, the Examiner cited col. 9, lines 25-56 of Venkatesan. However, col. 9, lines 25-56 of Venkatesan make clear that the digital signatures and establishment of chains of trust relate to "components of the O/S and particularly throughout enforcer 600 and DRM system 456," not between software products, publishers, and in some embodiments, certificate authorities, as claimed. Accordingly, Venkatesan fails to teach the cooperation of elements in claim 1 that provide for the delivery of secure software license information.

Therefore, it is respectfully submitted that independent claim 1 is allowable over Venkatesan for at least these reasons. Independent claims 12, 16, and 24, include similar recitations and are allowable for lease the same reasons as claim 1.

In view of the foregoing, it is submitted that claims 1-26 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-26 as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
STRATEGIC PATENT GROUP

April 24, 2006
Date

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 969-7474